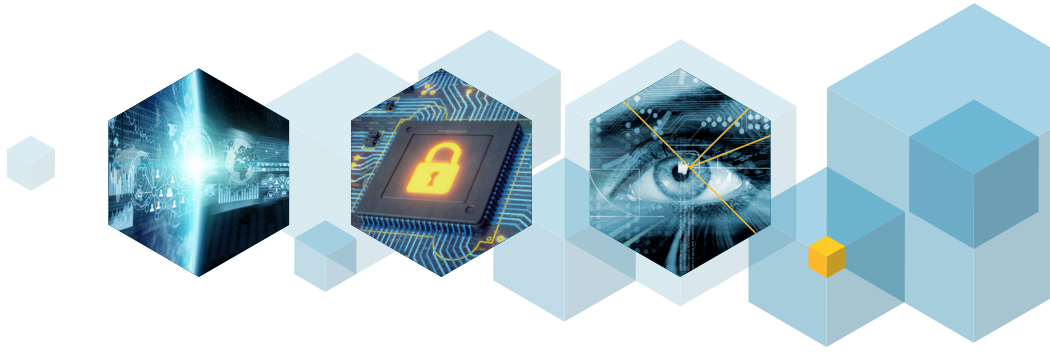
ILNAS

TRUST SERVICES
UNDER THE eIDAS REGULATION

Version 1.0 · June 2018



TRUST SERVICES
UNDER THE eIDAS REGULATION

Version 1.0 · June 2018

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

Contents

1. Introduction

Trust in the digital world is essential for making individuals and organizations use and adopt electronic services. Such services allow their users, for instance, to sign electronic documents with the help of electronic signatures, or to authenticate the website they are connecting to. Moreover, users may want to make sure that the integrity of electronic data that they store (e.g., electronically signed contracts, logging events) is preserved and that the data can be traced back to a particular point in time establishing evidence that the data existed at that time.

In this document we focus on the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation) [18], which introduces a range of "trust services" that can increase trust in electronic transactions.

The eIDAS Regulation [18] entered into force on 17 September 2014 and became applicable on 1 July 2016 (except for certain articles). The eIDAS Regulation replaces the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [37] (the eSignature Directive). As a Regulation of the European Union, it is directly applicable in all the EU Member States and hence also in Luxembourg.

The eIDAS Regulation mainly covers the following topics:

- **Electronic identification**: The eIDAS Regulation sets out conditions for EU Member States under which *electronic identification means*[1], issued in a EU Member State, have to be recognised in another EU Member State to access public online services and how to notify electronic identification schemes.

- **Trust services**: The eIDAS Regulation provides a legal framework for a range of trust services, including certificates for electronic signatures, certificates for electronic seals, certificates for website authentication, time stamp services, electronic registered delivery services, preservation services for electronic signatures/ seals, and validation services for electronic signatures/seals. In particular, it specifies security requirements applicable to trust service providers, requirements for qualified trust services providers, as well as the missions of the supervisory body.

- **Electronic documents**: The eIDAS Regulation dedicates a chapter to electronic documents, that is, any content stored in electronic form [18]. The chap-

[1] Under Article 3 (2) of the eIDAS Regulation, "electronic identification means" is defined as "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service" [18].

ter on electronic documents consists of one article which states that electronic documents benefit from the principle of non-discrimination as evidence in legal proceedings. This principle ensures that an electronic document is not denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form [18, Article 46]. Hence, in the European Union, a judge cannot reject an electronic document as evidence solely on the grounds that it is in electronic form. He may however reject the document on other grounds such as the lack of authenticity or the lack of integrity of the document.

This document focuses on trust services. Electronic identification and electronic documents are out of scope of this document.

The goal of the eIDAS Regulation in relation to trust services is to strengthen the trust of individuals as well as organizations in electronic transactions:

> "This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union". [18, Recital 2]

To enhance consumers' trust in electronic transactions, the eIDAS Regulation introduces the notions of "qualified" trust services (e.g., qualified electronic time stamps services, qualified electronic registered delivery services) which can be provided by "qualified" trust service providers. Compared to trust service providers who provide non-qualified trust services, "qualified" trust service providers need to meet further and stricter requirements. For example, qualified trust service providers have to be audited at their own expense at least every two years by a conformity assessment body. The supervision mechanism for qualified trust service providers introduced by the eIDAS Regulation guarantees a high level of security of the supervised qualified trust service providers and the qualified trust services that they provide, which in turn strengthens consumer trust in these qualified trust services.

In this document we provide incentives to the market to use trust services, and, in particular, qualified trust services.

The ***I**nstitut **L**uxembourgeois de la **N**ormalisation, de l'**A**ccréditation, de la **S**écurité et qualité des produits et services* (ILNAS), a public administration under the supervision of the Minister of the Economy of Luxembourg, is Luxembourg's supervisory body for trust service providers that are established in Luxembourg (see, [33]). In this context, ILNAS is in charge of the supervision of trust service providers and the trust services that they provide with respect to the requirements of the eIDAS Regulation.

2. Trust Services

The goal of this chapter is to inform the reader about the different trust services introduced by the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation) [18], to present the supervision scheme for qualified trust service providers that is applied by the Digital Trust Department of ILNAS, and to indicate incentives for using trust services.

This chapter is organized as follows. In Section 2.1 we highlight the main differences between the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [37] (the eSignature Directive) and the eIDAS Regulation. We present the different classes of electronic signatures and electronic seals in Section 2.2. In the latter section we also cover legal aspects of electronic signatures and seals. Then, in Section 2.3, we present the non-qualified and qualified trust services introduced by the eIDAS Regulation and indicate incentives for using them. In particular, we discuss in Section 2.3.3 remote signature services which provide a convenient way for users to electronically sign or seal documents. The supervision scheme of the Digital Trust Department of ILNAS is described in Section 2.4. Finally, in Section 2.5, we provide information on national trusted lists and on the European List of Trusted Lists, which includes pointers to the different national trusted lists.

2.1. Comparison between the eSignature Directive and the eIDAS Regulation

The eSignature Directive established a legal framework for electronic signatures. As a Directive, it had to be transposed into national law by the 28 Member States of the European Union, which led to differences in national legislation (e.g., regarding the supervision of the certification authorities who issue certificates for electronic signatures). In addition, the eSignature Directive had the following limitations:

- It only established a legal framework for electronic signatures, while other trust services emerged in certain EU Member States (e.g., the provision of electronic time stamps) and were non-regulated at EU level;
- Qualified electronic signatures were not recognized as such across borders within the European Union;

- In most EU Member States, including Luxembourg, advanced electronic signatures (and hence also qualified electronic signatures) could only be created if the user was under the sole control of his private signature key; the private signature key being stored locally on a physical device (e.g., a smart card, a USB stick) in possession of the user. This excluded the possibility of creating *remote* qualified signatures where the private signature key is managed by a trust service provider.

The eIDAS Regulation harmonizes the requirements for qualified trust service providers established in the European Union and the qualified trust services they can provide and promotes the adoption and use of such services, in particular, due to the cross-border recognition of qualified electronic signatures, seals, and time stamps in all the EU Member States. Compared to the eSignature Directive, the eIDAS Regulation is directly applicable in all the 28 EU Member States and does not need to be transposed into national law.

The eIDAS Regulation addresses the above limitations as follows:

- **Legal framework for several trust services.** Whereas the eSignature Directive only provided a legal framework for electronic signatures, the eIDAS Regulation provides a legal framework for additional trust services including electronic signatures, seals, timestamps, registered delivery services, preservation services for electronic signatures/seals, validation services for electronic signatures/seals, and certificates for website authentication.

- **Cross-border recognition of qualified electronic signatures, seals, and timestamps.** The eIDAS Regulation regulates the cross-border recognition of qualified electronic signatures, seals, and timestamps within the European Union. For instance, a qualified electronic signature, based on a qualified certificate for electronic signatures that has been issued by a qualified trust service provider in one Member State is recognized as a qualified electronic signature in all other Member States.

- **Relaxation of a requirement for advanced electronic signatures.** One of the requirements for "advanced electronic signatures" has been relaxed as it now states that "it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control" [18, Article 26]. This allows for advanced electronic signatures (and hence also qualified electronic signatures) to be created using remote signature services, where a trust service provider holds the private signature key of the user and only the user can activate his private signature key, for example, via his mobile phone.

Certificates for electronic signatures can only be issued to natural persons. Under the eSignature Directive, certificates for electronic signatures were issued to natural or legal persons. However, under the eIDAS Regulation, certificates for electronic signatures can only be issued to natural persons. The Regulation introduces the new concept of "certificates for electronic seals" which can be issued to legal persons. A

legal person can use an electronic seal to ensure the origin and integrity of data such as electronic documents.

Implementing acts related to trust services. The European Commission has adopted the following implementing acts in relation to trust services:

- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services [10],
- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [8],
- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [9],
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [11].

2.2. Electronic signatures and seals

2.2.1. Electronic signatures

The eIDAS Regulation distinguishes between three different classes of electronic signatures, namely the class of electronic signatures, the class of advanced electronic signatures, and the class of qualified electronic signatures.

An *electronic signature* is defined in the eIDAS Regulation as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign" [18], where the signatory is a natural person who creates electronic signatures.

The broad class of *electronic signatures* includes, for example,

- scanned signatures, and
- email signatures, that is, content that is added at the end of an email and which typically includes the name of a person, contact details, and a company logo.

A subclass of the class of electronic signatures is the class of *advanced electronic signatures*. According to Article 3(11) of the eIDAS Regulation, an advanced electronic signature is an electronic signature that meets the requirements of Article 26 of the eIDAS Regulation [18], that is: "(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable".

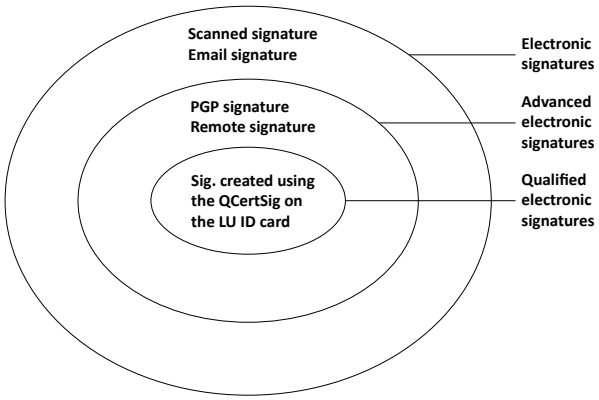


Figure 2.1.: Venn diagram of electronic signature classes and examples.

Digital signatures[1], which are based on public-key cryptography, can satisfy the requirements on advanced electronic signatures given in the eIDAS Regulation.

A user U with private/public key pair (sk, pk) can digitally sign data (e.g., an electronic document) using his private key sk. Any other party can verify that a given digital signature of user U on certain data is a valid signature using the corresponding public key pk.

The private signature key that the user uses to create a digital signature corresponds to the electronic signature creation data; it can be stored, for example, on a smart card or on a USB stick, under the control of the user. The private signature key can also be managed and stored by a trust service provider who offers remote signing services; the private key can be activated by the user to create digital signatures via a secure authentication process between the user and the remote signing service.

Digital signatures are used to ensure the authenticity and integrity of data (e.g., electronic documents, emails, software). Moreover, it is difficult for a natural person who created a digital signature on data to subsequently deny having created the signature (non-repudiation). In that sense, they provide higher security guarantees than simple electronic signatures that do not belong to the class of advanced electronic signatures.

The following types of signatures are examples of advanced electronic signatures:

- digital signatures created by using a private key for which a certificate for electronic signatures on the corresponding public key has been issued by a trust service provider,

[1] A digital signature is "data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient" [29].

- digital signatures created by using a private key stored on a smart card which also contains a qualified certificate for electronic signatures on the corresponding public key,
- digital signatures created remotely by a user whose private key and corresponding certificate for electronic signatures are managed by a trust service provider (this type of service is often called "remote signing service").
- digital signatures created by using a PGP private key (web of trust model).

The class of *qualified electronic signatures* contains all advanced electronic signatures that have been created by a qualified electronic signature creation device (QSigCD), and which are based on qualified certificates for electronic signatures that have been issued by a qualified trust service provider [18]. Qualified electronic signatures provide even stronger security guarantees than advanced electronic signatures as they (a) have to be created by a device that has been certified to satisfy the requirements in Annex II of the eIDAS Regulation, (b) are based on qualified certificates for electronic signatures and (c) those qualified certificates are issued by a qualified trust service provider. The European Commission maintains a list containing QSigCDs (see [15]).

A concrete example of a qualified electronic signature is

- a digital signature created by using the private key associated to the qualified certificate for electronic signatures contained in the Luxembourgish identity card issued under the law of 19th of June 2013 on the identification of natural persons, as amended [32] [2].

A qualified electronic signature cannot only be created via the use of smart cards that have been certified as QSigCDs, but also remotely via a hardware security module (HSM) that has been certified as remote QSigCD and under the control of a qualified trust service provider. Standards with requirements for systems that offer remote digital signatures as a service are currently being developed by the European Committee for Standardization (CEN). We refer the reader to Section 2.3.3 for details on remote signature services.

2.2.2. Electronic seals

As already mentioned in Section 2.1, electronic signatures can only be created by natural persons. Legal persons have the possibility to create electronic seals on data (e.g., electronic documents, software code) to ensure its integrity and authenticity.

Similar to the classification of electronic signatures, the eIDAS Regulation distinguishes between three different classes of electronic seals, namely the class of electronic seals, the class of advanced electronic seals, and the class of qualified electronic seals (see also Figure 2.2).

[2] Note that the Luxembourgish identity card contains two public-key certificates, one qualified certificate for electronic signatures and one certificate for authentication purposes (see, [32]).

An *electronic seal* is defined in the eIDAS Regulation as "data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity" [18]. Compared to electronic signatures, electronic seals can only be created by legal persons, not by natural persons.

A subclass of the class of electronic seals is the class of *advanced electronic seals*. According to Article 3(26) of the eIDAS Regulation, an *advanced electronic seal* is an electronic seal that meets the requirements of Article 36 of the eIDAS Regulation [18], that is: "(a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable", where the "creator of a seal" is defined in the eIDAS Regulation as the legal person who creates the seal.

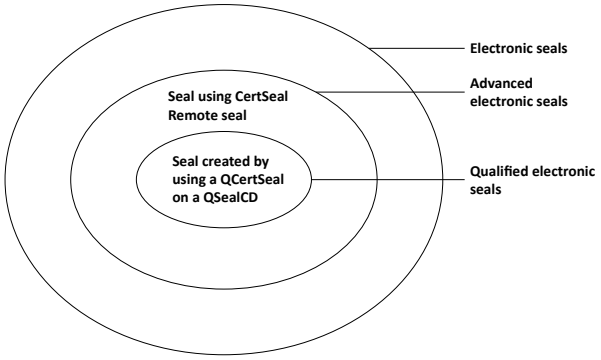


Figure 2.2.: Venn diagram of electronic seal classes and examples.

Digital signatures can satisfy the requirements above. The following types of seals are examples of advanced electronic seals:

- digital signatures created by using a private key for which a certificate for electronic seals (CertSeal) on the corresponding public key has been issued by a trust service provider,
- digital signatures created remotely by a legal person whose private key and corresponding certificate for electronic seals are managed by a trust service provider (this type of service is often called "remote sealing service").

The class of *qualified electronic seals* contains all advanced electronic seals that have been created by a qualified electronic seal creation device (QSealCD), and which are based on qualified certificates for electronic seals (QCertSeal) that have been issued by a qualified trust service provider [18]. Qualified electronic seals provide even stronger security guarantees than advanced electronic seals as they (a) have to be created by a device that has been certified to satisfy the requirements in Annex II of the eIDAS Regulation, (b) are based on qualified certificates for electronic seals and (c) those

qualified certificates are issued by a qualified trust service provider. Note that the list published by the European Commission also contains QSealCDs (see [15]).

2.2.2.1. Applications

Electronic seals can be used by legal persons for various applications.

- Universities can use electronic seals to guarantee the origin and integrity of electronic versions of the diplomas of their students [40]. Future employers of the students can hence readily verify the authenticity of the diplomas.
- Companies can use electronic seals to guarantee the authenticity of invoices that they send to their clients electronically. The verification of the electronic seal on the invoice allows the client to have certainty that the invoice indeed originates from the company and has not been modified.
- Software companies can create advanced electronic seals on software before they release it. This allows users to verify the software's integrity and the source where it originates from. Any modification to the software by a malicious party would result in an invalid signature on the malicious software.
- Laws and regulations that are published online can be protected against accidental or malicious tampering by using electronic seals. For example, the *Ministère d'Etat* of Luxembourg created an advanced electronic seal on the Grand-Ducal Regulation of 22 May 2017, published in the *Journal officiel du Grand-Duché de Luxembourg* and available electronically on the Legilux website[3]. We show in Figure 2.3 some information about the certificate for electronic seals associated with the private key that has been used to create the seal on the Grand-Ducal Regulation; this information is obtained when validating the electronic seal on the PDF document with Adobe® Acrobat® Reader® software.
- Supervisory bodies of the EU Member States who are responsible for the supervision of qualified trust service providers may use electronic seals instead of electronic signatures to guarantee the integrity and authenticity of their respective national trusted lists (see Article 22 paragraph (2) of the eIDAS Regulation).

2.2.2.2. Technical aspects

We illustrate the similarities and differences between advanced electronic signatures and advanced electronic seals through an example. Suppose that, to ensure the integrity of a document, a company generates a digital signature on the document by using the private key for which a certificate for electronic seals on the corresponding public key has been issued by a trust service provider. Then this digital signature can be considered as an advanced electronic seal on the document (under the assumption that the private key has not been compromised).

[3] http://legilux.public.lu/eli/etat/leg/rgd/2017/05/22/a563/jo

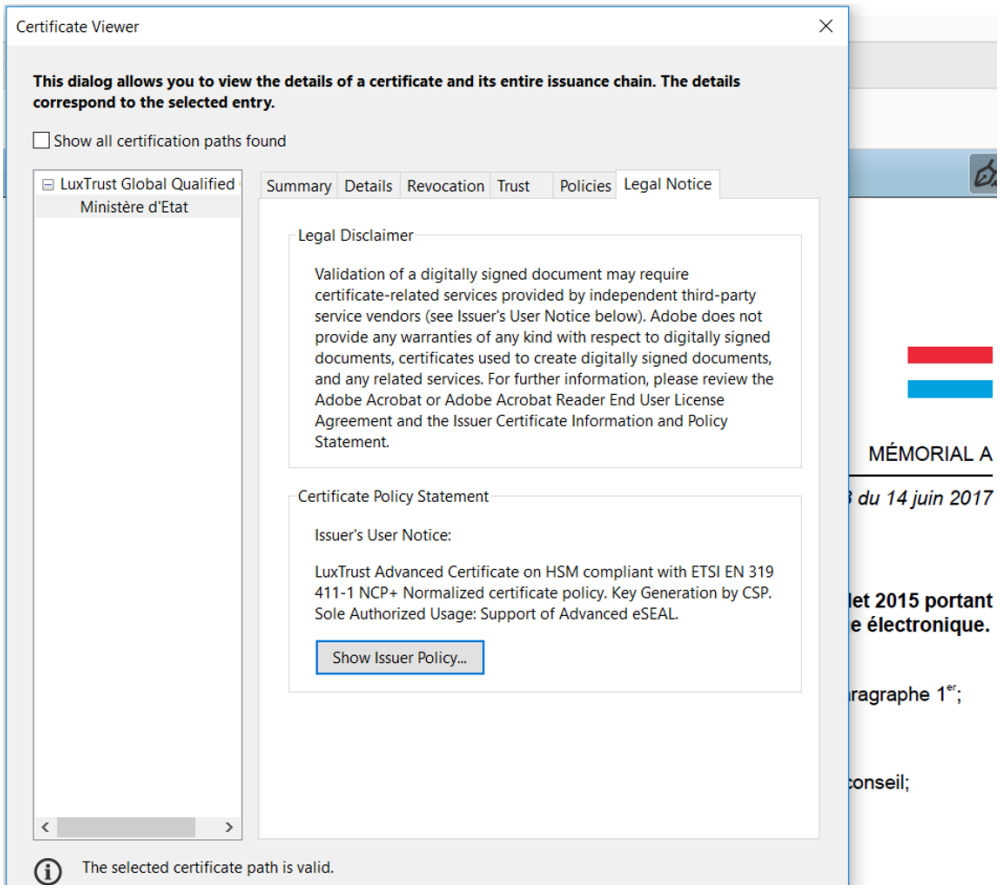


Figure 2.3.: Advanced electronic seal on Grand-Ducal Regulation of 22 May 2017. Screenshot. 29/11/2017

Similarity to advanced electronic signatures. Similar to advanced electronic signatures, advanced electronic seals can be realized through digital signatures as they satisfy the requirements on advanced electronic seals given in the eIDAS Regulation. Recall that digital signatures are based on public-key cryptography; a private key is used to digitally sign data and a corresponding public key is used to verify that a given signature is a valid signature on certain data.

Differences to advanced electronic signatures. Whereas certificates for electronic signatures can only be issued to natural persons, certificates for electronic seals can only be issued to legal persons. Thus, a certificate for electronic seals binds the identity of a legal person (e.g., name of a company and its registration number as stated in the official records) to a public key.

The action of creating an electronic seal on behalf of a legal person can be triggered, for example, by a natural person. In this case, as it might be more difficult to relate a physical person to an electronic seal created on data, it may be necessary for the legal person to implement technical or organizational measures to be able to identify the natural person who created the electronic seal on certain data. In particular, companies may want to keep track of the mapping between certificates for electronic seals (uniquely identifiable through a serial number) issued by a trust service provider and the natural persons to whom the company has assigned these certificates in order to actually create electronic seals on data.

2.2.3. Legal effects

Non-discrimination as evidence in legal proceedings. The eIDAS Regulation applies the principle of non-discrimination to electronic signatures, electronic seals, electronic time stamps, data sent and received using electronic registered delivery services, and electronic documents. Thus, in particular, electronic signatures and seals cannot be denied legal effect and admissibility as evidence in legal proceedings only on the grounds that they are in electronic form or that they do not meet the requirements for qualified electronic signatures or seals, respectively. Thus, for example, a judge cannot reject an electronic signature in a legal proceeding on the grounds that it is in electronic form; he may however reject the signature on other grounds (e.g., if there is evidence that the signature is not authentic or if there is a national law which mandates the use of qualified electronic signatures on a specific type of document).

Legal effect of qualified electronic signatures. As qualified trust service providers who issue qualified certificates for electronic signatures on qualified electronic signature creation devices (QSigCDs) have to meet all the applicable requirements in the eIDAS Regulation[4], qualified electronic signatures that have been created by these QSigCDs provide stronger security guarantees and higher legal certainty than non-qualified electronic signatures. Therefore, the eIDAS Regulation grants to qualified electronic signatures the equivalent legal effect of handwritten signatures [18, Article 25(2)].

Legal effect of qualified electronic seals. According to Article 35 paragraph (2) of the eIDAS Regulation [18], qualified electronic seals enjoy "the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked".

Recognition in all EU Member States of qualified electronic signatures and seals. The eIDAS Regulation regulates the cross-border recognition of qualified electronic signatures and seals on an EU level, which is particularly interesting for companies that carry out digital transactions in more than one EU Member State:

[4] In particular, the qualified trust service provider has to verify the identity of the natural person to whom the qualified certificate for electronic signatures is issued.

- Qualified electronic signatures based on qualified certificates for electronic signatures issued in one EU Member State are recognised as qualified electronic signatures in all other EU Member States [18, Article 25(3)].
- Qualified electronic seals based on qualified certificates for electronic seals issued in one EU Member State are recognised as qualified electronic seals in all other EU Member States [18, Article 35(3)].

2.3. Trust services under eIDAS

The scope of the eIDAS Regulation is larger than the one of the eSignature Directive as it not only covers the provision of certificates for electronic signatures, but also a variety of other trust services including the provision of certificates for electronic seals, the provision of certificates for website authentication, the creation of electronic timestamps, electronic registered delivery services, and the preservation of electronic signatures or seals.

2.3.1. Definition and description of trust services

Under Article 3 (16) of the eIDAS Regulation, a "trust service" is defined as "an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services" [18].

For a subset of these trust services, there are specific requirements in the eIDAS Regulation for them to be considered as "qualified trust services". Compared to trust service providers who only provide non-qualified trust services, trust service providers who intend to provide qualified trust services need to meet further and stricter requirements which are specified in the eIDAS Regulation (see Section 2.3.2).

In the following we describe some of the trust services in more detail. Qualified trust services and the requirements of those services will be addressed in Section 2.3.2.

2.3.1.1. Provision of certificates for electronic signatures

A *certificate for electronic signature* is an "electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person" [18, Article 3(14)]. In more technical terms, a certificate for electronic signature binds the identity of a natural person to a public key.

Certificates for electronic signature can be used by natural persons to sign data. More precisely, a natural person can create an electronic signature on data using the private key corresponding to the public key contained in the certificate, "mainly to express consent on the data the electronic signature is put" [12].[5]

2.3.1.2. Provision of certificates for electronic seals

A *certificate for electronic seal* is "an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person" [18, Article 3(29)]. Compared to a certificate for electronic signature, a certificate for electronic seal binds the identity of a legal person to a public key.

Certificates for electronic seals can be used by legal persons to ensure:

- the authenticity of data (i.e., the data originates from the legal person to whom the certificate has been issued), and
- the integrity of data (i.e., the data has not been modified),

while transmitted over a network or stored on some hardware. Furthermore, a legal person who creates an electronic seal based on a certificate for electronic seal on data cannot later on deny having created the seal (non-repudiation).

As a concrete example, suppose that a company would like to use certificates for electronic seals to ensure the authenticity and integrity of invoices that they send to their clients via email. The company can create electronic seals on the invoices using the private key which corresponds to the public key contained in the certificate; and the company's clients to whom the invoices are sent can verify whether the invoices indeed originate from the claimed company and that they have not been modified during the transmission using the public key included in the certificate. Note however that electronic seals on data do not ensure the data's confidentiality. Different cryptographic mechanisms need to be used to protect the confidentiality of the data during the transmission. Further applications where certificates for electronic seal can be used are provided in Section 2.2.2.1 and in Recital (65) of the eIDAS Regulation [18].

As recommended by the European Commission, when a legal person uses several certificates for electronic seals, it should set up an "internal control mechanism ensuring that only the natural persons entitled to act on behalf of the legal entity can make use of the electronic seals (push the button on behalf of the legal entity)" [12]. Internal control mechanisms may include adapting existing information security policies and procedures, requiring employees to sign a policy regarding the use of certificates for electronic seals, maintaining an internal table which maps the identity of the natural person entitled to act on behalf of the legal entity to a certificate (e.g., via its serial number), and organizing specific awareness training for those employees to whom the certificates for electronic seals have been distributed.

[5] Recall that under the eSignature Directive "the electronic signature, which could also be used by legal persons, was defined as a means for authentication" [12].

2.3.1.3. Provision of certificates for website authentication

A *certificate for website authentication* is "an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued" [18, Article 3 (38)].

Certificates for website authentication can be used to authenticate a website (i.e., to confirm that the entity behind the website is who it claims to be). These certificates can be used in the TLS protocol to secure the communication between a web server and a web browser. If a certificate for website authentication is used on the server side, the TLS protocol provides authentication of the server, integrity and confidentiality of the information transmitted between the web server and the browser.

2.3.1.4. Creation of electronic timestamps

According to Article 3(33) of the eIDAS Regulation, an electronic timestamp is "data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time" [18]. Time stamps are usually used to bind data to a particular point in time in order to be able to prove later on that the data (e.g., scientific publications, electronically signed contracts, electronic files, intellectual property) existed at that point in time and is bound to a certain identity.

Time stamps can be created by a central Time Stamping Authority (TSA) who acts as a trusted third party. The Time Stamping Authority creates time stamps on some data to establish evidence indicating that the data existed at that point in time. The document RFC 3161 "Time-Stamp Protocol" (2001) provides requirements for Time Stamping Authorities and describes a time-stamp protocol between an entity who requests a time stamp and a Time Stamping Authority. These requirements include, for example, that Time Stamping Authorities have to use a trustworthy source of time and that they only time-stamp a hash of the data to be timestamped. TSA's describe the practices that they employ to generate time stamps in their policies.

Under Article 41 (1) of the eIDAS Regulation, electronic time stamps benefit from a non-discrimination clause as evidence in legal proceedings, meaning that a judge cannot reject them as evidence only on the grounds that they are in electronic form or that they do not meet the requirements of qualified electronic time stamps.

2.3.1.5. Validation of electronic signatures/seals

According to Article 3(41), the validation of an electronic signature/seal refers to the process of verifying and confirming that an electronic signature or a seal is valid [18].

In Figure 2.4 we illustrate a signature validation process between a user and a trust service provider (TSP) who provides a signature validation service. We assume a secure channel between the user and the TSP in order to ensure the confidentiality and integrity of the transmitted messages as well as entity authentication of the TSP's server. The signature validation works as follows:

1. The user first sends a signature validation request to the TSP via the signature validation client. This request typically includes an electronic document as well as a signature on an electronic document.

2. Upon receipt of the request, the TSP executes the signature validation application, which may require accessing information from external sources (e.g., other TSPs, the EU LOTL (see Section 2.5.2)). The signature validation application may perform different checks, such as:
   - **Revocation check:** the check whether the certificate was not revoked at the time of signing,
   - **Expiration check:** the check whether the certificate was not expired at the time of signing,
   - **Digital signature check:** the cryptographic verification whether the digital signature is a valid signature on the electronic document.

3. The TSP returns the signature validation result, via the signature validation application, to the user. The validation result typically contains an indication as to whether or not the signature is a valid signature on the document and may contain additional information such as information about the type of signature (advanced or qualified) or the reasons why the signature is invalid.

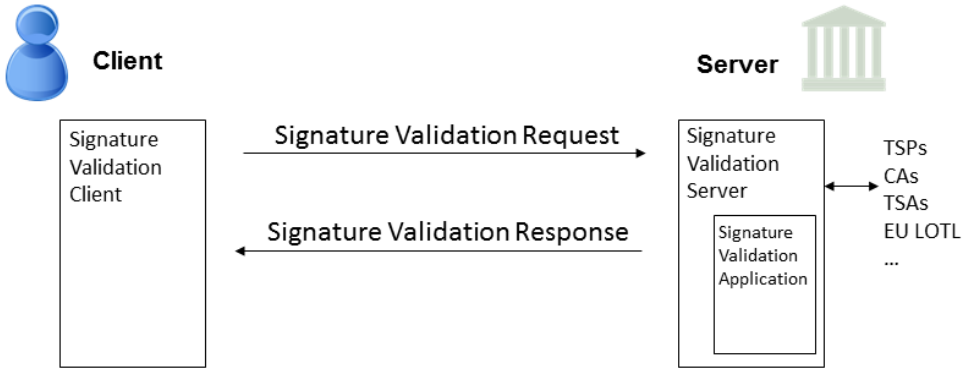


Figure 2.4.: Signature validation process (see also [22])

Standards. To date there are only very few standards on signature validation (e.g., [21] (currently under revision)). In addition, none of the existing standards covers all of the requirements for qualified validation services of qualified electronic signatures/seals, which we discuss in Section 2.3.2.5. The standardization organisation ETSI is currently developing further standards and technical specifications for signature validation services. In Table 2.1 we provide a list of documents to be developed by the Specialist Task Force 524:

TS 119 102-2	Procedures for creation and validation of AdES Digital Signatures. Part 2 - Signature Validation Report
TS 119 441	Policy requirements for TSPs providing signature validation services
TS 119 442	Protocol for TSPs providing signature validation services

Table 2.1.: Standards to be developed by STF 524 [2]

2.3.1.6. Preservation of electronic signatures/seals

The eIDAS Regulation addresses the need for long-term preservation of electronic signatures and seals in its Recital (61):

> "This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes" [18].

Long-term preservation of electronic signatures/seals aims to ensure the legal verifiability of electronic signatures/seals over time. A preservation service for electronic signatures/seals preserves the result of a signature or seal validation, at a certain point in time, over long periods of time during which the technological state of the art might evolve; for example, attacks on cryptographic hash functions or algorithms might be found [41], vulnerabilities in cryptographic libraries might be discovered [35], physical storage media, hardware or software might become obsolete [36].

Furthermore, if an electronic signature/seal is created by using a private key for which a certificate for electronic signatures/seals on the corresponding public key has been issued by a trust service provider, then the validity of the electronic signature/seal depends on the status of the certificate. A certificate is only valid during a limited time frame (e.g., two years) after which it will expire. During this time frame the issuing trust service provider may revoke the certificate due to some event such as the compromise of the associated private key. Hence, the validation of an electronic signature based on a certificate for electronic signatures may yield "valid" today, but may yield "invalid" at some point in the future due to the change of status of the certificate.

Comparison between preservation of electronic signatures/seals and electronic archiving:

- Preservation of electronic signatures/seals is a trust service under the eIDAS Regulation, whereas electronic archiving is not a trust service under the eIDAS Regulation. Note however that EU Member States may define electronic archiving as a trust service at the national level (see also Recital (25) of the eIDAS Regulation [18]).
- In contrast to preservation services for electronic signatures/seals, electronic archiving targets electronic documents and aims at ensuring their long-term availability and integrity. Electronic documents may or may not be signed or sealed.

In 2017 ETSI published a special report on a framework for standardization of long-term data preservation services, including preservation of digital signatures [43]. Topics covered in the report include models for long-term data preservation services, basic preservation techniques (e.g., time stamps, AdES digital signatures, Evidence Record Syntax), and a proposal for a framework of standards for data preservation. In

particular, the report provides an overview of preservation mechanisms for preserving the validity status of digital signatures.

2.3.1.7. Electronic registered delivery services (ERDS)

According to Article 3(36) of the eIDAS Regulation, an *electronic registered delivery service* is "a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations" [18].

Registered electronic mail. A Registered Electronic Mail (REM) service can be considered as a specific type of Electronic Registered Delivery service. A registered electronic mail service is defined in the ETSI Special Report 019 050 on a framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures as an "electronic registered delivery service based on electronic mail as the underlying technology" [20]. In contrast to traditional email services, registered email services provide to their users a set of evidences, which may include a proof of sending the email, a proof of delivering the email to the intended recipient, and a proof of receiving the email.

Legal effect of an electronic registered delivery service. The eIDAS Regulation applies the principle of non-discrimination to data sent and received using an electronic registered delivery service. Thus, data sent and received using such a service cannot be denied legal effect and admissibility as evidence in legal proceedings on the grounds that it is in electronic form or that it does not meet the requirements for qualified electronic registered delivery services [18, Article 43(1)]. Thus, for example, a judge cannot reject an email, sent with a REM service, in a legal proceeding on the grounds that it is in electronic form; he may however reject the email on other grounds.

Upcoming ETSI standards. ETSI is currently working on standards for Electronic Registered Delivery and Registered Electronic Mail, which specify, among others, policy and security requirements for Electronic Registered Delivery service providers as well as for Registered Electronic Mail service providers. In Table 2.2 we provide a list of the standards to be developed by the Specialist Task Force 523.

2.3.2. Qualified trust services

In this chapter, the different qualified trust services will be presented. In particular, the legal implications of the qualified trust services will be discussed. Furthermore, we describe incentives to the market for using qualified trust services.

The eIDAS Regulation regulates the following nine qualified trust services for which there are applicable requirements in the eIDAS Regulation:

1. Provision of qualified certificates for electronic signatures

ETSI EN 319 522	Electronic Registered Delivery Services
ETSI EN 319 532	Registered Electronic Mail (REM) Services
ETSI EN 319 521	Policy and Security Requirements for Electronic Registered Delivery Service Providers
ETSI EN 319 531	Policy and Security Requirements for Registered Electronic Mail Service Providers
ETSI EN 319 524	Testing Conformance and Interoperability of Electronic Registered Delivery Services
ETSI EN 319 524	Testing Conformance and Interoperability of Registered Electronic Mail Services
ETSI EN 319 500	Guidance on the use of standards for Trust Application Service Providers

Table 2.2.: Standards to be developed by STF 523 [1]

2. Provision of qualified certificates for electronic seals
3. Provision of qualified certificates for website authentication
4. Qualified electronic time stamps services
5. Qualified validation service for qualified electronic signatures
6. Qualified validation service for qualified electronic seals
7. Qualified preservation service for qualified electronic signatures
8. Qualified preservation service for qualified electronic seals
9. Qualified electronic registered delivery services

Note that qualified trust services can only be provided by "qualified trust service providers". According to the eIDAS Regulation, a "qualified trust service provider" is "a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body" [18, Article 3(20)].

2.3.2.1. Provision of qualified certificates for electronic signatures

According to the eIDAS Regulation, a qualified certificate for electronic signature is a "certificate for electronic signatures that is issued by a qualified trust service provider and meets the requirements laid down in Annex I" [18, Article 3(15)]. Recall that certificates for electronic signatures can only be issued to natural persons.

Annex I of the eIDAS Regulation contains requirements on the certificate profile of qualified certificates for electronic signatures. In particular, they have to contain the identity of the trust service provider, the identity of the signatory (either a name or

a pseudonym), a public key, and an indication that the certificate has been issued as a qualified certificate for electronic signature. The indication that the certificate has been issued as a qualified certificate for electronic signatures is commonly included in the certificate extension field "Qualified Certificate Statements" via the object identifier (OID) 0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) (QcCompliance statement) in combination with the OID 0.4.0.1862.1.6.1 (id-etsi-qct-esign) (QcType statement) [23].

Compared to non-qualified certificates for electronic signatures, qualified certificates for electronic signatures can only be issued by qualified trust service providers that have been granted the qualified status for this trust service by the national supervisory body, which is indicated on the national trusted list. Under the eIDAS Regulation, national trusted lists have a constitutive value as they present the only reliable source to verify whether a given trust service provider and its trust service have the "qualified" status (see, Section 2.5.1). We refer the reader to Section 2.4.1 for the procedure to be followed by trust service providers established in Luxembourg who would like to offer qualified trust services.

As explained in Section 2.2.1, qualified certificates for electronic signatures can be used to create advanced electronic signatures or qualified electronic signatures (if the private key related to the certified public key resides in a QSigCD).

Incentives. Qualified certificates for electronic signatures where the private key related to the certified public key resides in a QSigCD include can be used, for example, in the following cases:

- The creation of qualified electronic signatures on electronic documents (e.g., contracts) where high legal or financial risks are involved.
- The creation of qualified electronic signatures on electronic documents where cross-border recognition of the electronic signature in other EU Member States is relevant.
- The creation of qualified electronic signatures on electronic transactions to enhance their security. In this context, the European Commission states in their Communication "Consumer Financial Services Action Plan: Better Products, More Choice" [24] that "The legal certainty and validity of qualified eSignatures, as provided for under eIDAS, could also enhance the security of electronic transactions. This should work across borders and across sectors, and it should have the same legal effect as traditional paper based processes" [24, Section 4.2.1 on remote identification].
- Legal and regulatory requirements: For example, the measure 10.1.6 of the Grand-Ducal Regulation of September 21st 2017 related to electronic archiving [34] recommends users of the dematerialisation or conservation system to use a qualified signature or mechanisms providing equivalent guaranties to validate the internal documents that are necessary for proving correct the functioning of the electronic archiving management system [34, Annex II Section 10.1.6].

- Standards that require or recommend the use of qualified certificates for electronic signatures.

2.3.2.2. Provision of qualified certificates for electronic seals

According to the eIDAS Regulation, a qualified certificate for electronic seal is a "certificate for an electronic seal that is issued by a qualified trust service provider and meets the requirements laid down in Annex III" [18, Article 3(30)]. Recall that certificates for electronic seals can only be issued to legal persons.

Annex III of the eIDAS Regulation contains requirements on the certificate profile of qualified certificates for electronic seals. In particular, they have to contain the identity of the trust service provider, the identity of the creator of the seal (name and registration number as stated in the official records), a public key, and an indication that the certificate has been issued as a qualified certificate for electronic seal. The indication that the certificate has been issued as a qualified certificate for electronic seal is commonly included in the certificate extension field "Qualified Certificate Statements" via the object identifier (OID) 0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) (QcCompliance statement) in combination with the OID 0.4.0.1862.1.6.2 (id-etsi-qct-eseal) (QcType statement) [23].

As explained in Section 2.2.1, qualified certificates for electronic seals can be used to create advanced electronic seals or qualified electronic seals (if the private key related to the certified public key resides in a QSealCD).

Incentives. Incentives for using qualified certificates for electronic seals include, for example:

- Legal and regulatory requirements: for example, requirements in the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [38] (commonly called PSD2) and associated Regulatory Technical Standards on authentication and communication. In particular, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing PSD2 with regard to regulatory technical standards (RTS) for strong customer authentication and common and secure open standards of communication [14] requires that "For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation [14, Article 34(1)]. For further information, we refer the reader to Appendix A.1.
- Tallinn declaration on eGovernment (signed by the EU Member States and the EFTA countries): The signatories of the Tallinn declaration on eGovernment

committed themselves to undertaking a set of policy action lines in their respective countries. In particular, they committed themselves to securing the digital public services they provide, in particular by integrating the use of qualified certificates for electronic seals [3].

- Standards that require or recommend the use of qualified certificates for electronic seals.

In particular, qualified certificates for electronic seals where the private key related to the certified public key resides in a QSealCD can be used, for example, in the following cases:

- The creation of qualified electronic seals on data where high legal, financial, or strategic risks are involved.
- The creation of qualified electronic seals on data where cross-border recognition of the electronic seal in other EU Member States is relevant.
- The creation of qualified electronic seals on electronic transactions to enhance their security.
- Legal and regulatory requirements.
- Standards.

2.3.2.3. Provision of qualified certificates for website authentication

According to the eIDAS Regulation, a qualified website authentication certificate (QWAC) is "a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV" [18, Article 3(39)]. Under the eIDAS Regulation, qualified certificates for website authentication can be issued to both natural and legal persons.

Annex IV of the eIDAS Regulation contains requirements on the certificate profile of qualified certificates for website authentication. In particular, they have to contain the identity of the trust service provider, the identity of the natural or legal person to whom the certificate is issued, an indication that the certificate has been issued as a qualified certificate for website authentication, and the domain name(s) operated by the person to whom the certificate is issued. The indication that the certificate is issued as a qualified certificate for website authentication is commonly included in the certificate extension field "Qualified Certificate Statements" via the object identifier (OID) 0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) (QcCompliance statement) in combination with the OID 0.4.0.1862.1.6.3 (id-etsi-qct-web) (QcType statement) [23]. Astonishingly, compared to the requirements in Annex I and Annex III, there is no requirement in Annex IV that the qualified certificate for website authentication contains a public key (in other words, website authentication validation data); it is however implicitly clear that website authentication certificates also include a public key.

We refer the reader to Appendix A.2 for a comparison between qualified certificates for website authentication and extended validation (EV) certificates.

Incentives. Incentives for using qualified certificates for website authentication include, for example:

- Legal and regulatory requirements: for example, requirements in the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [38] (commonly called PSD2) and associated Regulatory Technical Standards on authentication and communication. In particular, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing PSD2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [14] requires that "For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation [14, Article 34(1)]. For further information, we refer the reader to Appendix A.1.

- Tallinn declaration on eGovernment (signed by the EU Member States and the EFTA countries): The signatories of the Tallinn declaration on eGovernment committed themselves to undertaking a set of policy action lines in their respective countries. In particular, they committed themselves to securing the digital public services they provide, in particular by integrating the use of qualified certificates for website authentication [3].

- The appearance of a special symbol in the address bar of widely-used web browsers that clearly indicates that the certificate used by the visited website is a qualified certificate for website authentication. At the time of writing browsers do not indicate a special symbol for such certificates. They only display a green lock symbol in the address bar to indicate the trust status *according to the browser*. Thus, qualified trust service providers who offer qualified or non-qualified certificates for website authentication need to follow the procedures of the browsers (in addition to eIDAS-specific requirements) if they want their root certificate to appear in the trust list of the browser.

- Standards that require or recommend the use of qualified certificates for website authentication.

The availability and use of browser plugins that enable the visitor of a website to detect whether the website uses a qualified certificate for website authentication (that would otherwise require the manual inspection of the certificate) might also become an incentive for using qualified certificates for website authentication.[6]

[6] The A-SIT recently developed an addon for Mozilla Firefox that enables the user to verify whether a website uses a certificate for website authentication (indicated by a blue EU flag in the address bar of the browser) [6]. Further inspection of the icon allows the user to check whether the certificate has been issued as a qualified or as a non-qualified certificate for website authentication. The plugin is intended for demonstration purposes.

2.3.2.4. Qualified electronic time stamps services

Article 42 (1) of the eIDAS Regulation specifies the requirements for a time stamp to be considered as a qualified electronic time stamp: "A qualified electronic time stamp shall meet the following requirements: (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; (b) it is based on an accurate time source linked to Coordinated Universal Time; and (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method" [18].

The requirements above can be met by a timestamping service offered by a qualified trust service provider (QTSP), where the time stamps contain a digital signature of a Time Stamping Authority managed by the QTSP.

The legal effects of qualified electronic time stamps are that:

- they enjoy the presumption of accuracy of the date and the time they indicate and integrity of the data to which the date and time are bound [18, Article 41(2)], and that
- they are recognised as qualified electronic time stamps in all EU Member States, even though they are issued in one Member State [18, Article 41(3)].

Incentives. Incentives for using qualified time stamping services include, for example:

- The creation of qualified electronic time stamps on data where high legal, financial, or strategic risks are involved with regards to the existence of that data at some particular point in time (e.g., transactions, trade secrets, inventions).
- The creation of qualified electronic time stamps on data for which cross-border recognition of the time stamps in other EU Member States is relevant.
- The creation of qualified electronic time stamps on archived data in order to protect their integrity. Note however that the validity of the time stamps should be preserved over time (as technological changes may invalidate them).
- Regulatory Requirements: For example, in the context of electronic archiving, the Grand-Ducal Regulation of 21 September 2017 recommends to protect the integrity of internal documents (in particular, logging events) using qualified time stamping [34, Annex II Section 10.1.5].

2.3.2.5. Qualified validation service for qualified electronic signatures or seals

> "To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that

> can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level." [18, Recital (57)]

The objective of a validation service for qualified electronic signatures/seals is to confirm or deny that a given electronic signature/seal on data was a *qualified* electronic signature/seal on that data *at the time of signing*.

The eIDAS Regulation specifies requirements for:

- the qualified validation services for qualified electronic signatures/seals, and
- the validation process of qualified electronic signatures/seals.

In the following, we present both sets of requirements.

Requirements for qualified validation services for qualified electronic signatures/seals. According to Article 33(1) of the eIDAS Regulation [18], a qualified validation service for qualified electronic signatures has to satisfy the following requirements:

1. It may only be provided by a qualified trust service provider (QTSP);
2. The QTSP performs signature validation as specified in Article 32(1) of the eIDAS Regulation (see below);
3. The QTSP allows users of its service to receive the result of the validation process in an automated manner, which is reliable and efficient;
4. The validation result is electronically signed or sealed by the QTSP;
5. The electronic signature or seal on the validation result by the QTSP is an advanced electronic signature, respectively, an advanced electronic seal.

Similar requirements apply to qualified validation services for qualified electronic seals (see [18, Article 40]).

Requirements for the validation process of qualified electronic signatures/seals. Article 32(1) enumerates the conditions that have to be verified by the QTSP to determine whether or not a given electronic signature is a valid qualified electronic signature on a given document[7]:

[7] It is an interesting open question whether these requirements are sufficient from a security perspective. Would it be possible for an attacker to generate a valid qualified electronic signature on behalf of the legitimate signatory (e.g., by exploiting vulnerabilities (e.g., [35]) and backdating the time of signing of a document of the attacker's choice before revocation of the associated qualified certificate)? In the latter case, even though the requirements on advanced electronic signatures were met at the time of signing, they were not met at a later point in time when the attacker created a valid signature (backdated).

(a) "the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

(c) the signature validation data corresponds to the data provided to the relying party;

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(f) the electronic signature was created by a qualified electronic signature creation device;

(g) the integrity of the signed data has not been compromised;

(h) the requirements provided for in Article 26[8] were met at the time of signing" [18, Article 32(1)].

According to the eIDAS Regulation, an electronic signature on data is a valid qualified electronic signature on that data if and only if all of the above conditions are satisfied.

In addition to the above requirements, Article 32(2) requires that "The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues" [18].

Similar requirements apply to the validation process of qualified electronic seals (see [18, Article 40]).

Incentives. Incentives for using a qualified validation service for qualified electronic signatures or seals include, for example:

- The validation of qualified electronic signatures/seals by lawyers, notaries, judges, or insurance companies to verify whether or not a given signature/seal is a valid qualified electronic signature/seal on a specific electronic document.
- Legal and regulatory requirements.
- Standards.

[8] Recall that Article 26 of the eIDAS Regulation specifies the requirements for advanced electronic signatures.

2.3.2.6. Qualified preservation service for qualified electronic signatures or seals

Article 34 (1) of the eIDAS Regulation specifies the requirements for qualified preservation services for qualified electronic signatures: "A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period" [18]. Similar requirements also hold for qualified preservation services for qualified electronic seals [18, Article 40].

Incentives. Incentives for using a qualified preservation service for qualified electronic signatures or seals include, for example:

- The preservation of signed or sealed electronic documents (e.g., contracts, agreements) where high legal or financial risks are involved.
- The preservation of signed or sealed electronic documents which remain relevant over long periods of time (e.g., notarial acts).
- Legal and regulatory requirements.
- Standards.

At the time of writing there are no standards yet for qualified preservation services for qualified electronic signatures or seals.

2.3.2.7. Qualified electronic registered delivery services

According to Article 3(37) of the eIDAS Regulation, a *qualified electronic registered delivery service* is "an electronic registered delivery service which meets the requirements laid down in Article 44" [18].

Legal effects of a qualified electronic registered delivery service. The principle of non-discrimination of data sent and received using an electronic registered delivery service as evidence in legal proceedings also applies to data sent and received using a qualified electronic registered delivery services. Compared to non-qualified electronic registered delivery services, data sent and received using a qualified electronic registered delivery service enjoys "the presumption of:

- the integrity of the data,
- the sending of that data by the identified sender,
- its receipt by the identified addressee and
- the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service" [18, Article 43(2)].

Requirements for qualified electronic registered delivery services. Article 44(1) of the eIDAS Regulation specifies the following requirements for qualified electronic registered delivery services:

1. "they are provided by one or more qualified trust service provider(s);
2. they ensure with a high level of confidence the identification of the sender;
3. they ensure the identification of the addressee before the delivery of the data;
4. the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
5. any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;
6. the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp. In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers" [18, Article 44(1)].

Relation to registered postal mail. The eIDAS Regulation does not define an equivalence between qualified electronic registered delivery services and registered postal mail. However, Member States can establish this equivalence at the national level.

Incentives. Incentives for using a qualified electronic registered delivery service or a qualified registered electronic mail service include, for example:

- The equivalence with registered postal mail at the national level. This equivalence would imply that a qualified electronic registered delivery service (or a qualified registered electronic mail service) can be used whenever certain data are required to be sent via registered postal mail (unless there are specific national requirements which require the use of registered postal mail only).
- E-government and administrative simplification: Qualified electronic registered delivery services could be used by citizens and companies to interact with public administrations. For example, such a service could be used to submit tax declarations; the advantages would be a faster transmission to the public administration as well as the legal effects associated with the qualified registered delivery service (in particular, the presumption of the sending of the tax declaration by the identified sender and its receipt by the identified addressee).
- Legal and regulatory requirements.
- Standards.

2.3.3. Remote signing services

A remote signature service allows users to create remote electronic signatures, where the private signature keys of the users as well as the signature creation device are managed by a trust service provider on behalf of the signatory.

As explained in Section 2.1, the eSignature Directive did not allow the creation of remote advanced electronic signatures (and hence also qualified electronic signatures) where the users' private keys are managed by a trust service provider. The eIDAS Regulation addresses this issue by allowing the creation of remote advanced and qualified electronic signatures:

> "The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply." [18, Recital (52)].

Hence, under the eIDAS Regulation, qualified trust service providers can provide remote signing services to create qualified electronic signatures as long as the qualified trust service provider and the associated qualified trust service (namely, the provision of qualified certificates for electronic signatures) meet the applicable requirements in the eIDAS Regulation.

2.3.3.1. Remote qualified electronic signatures

Description of a remote signature creation process. In Figure 2.5 we illustrate a remote signature creation process between a user and a qualified trust service provider (QTSP) who provides a remote signing service.

Prior to using the remote signing service, the user needs to request a qualified certificate for electronic signature from the QTSP. The QTSP generates a new private/public key pair (sk, pk) for the user and creates a qualified certificate for electronic signature which binds the user's identity to the public key pk. The user's private key (sk) and the associated certificate are stored and managed by the QTSP on behalf of the user.

In the following we describe a signature creation process between a user and a qualified trust service provider who provides a remote signing service for the creation of qualified electronic signatures. We assume a secure channel between the user and the QTSP in order to ensure the confidentiality and integrity of the transmitted messages

as well as entity authentication of the QTSP. We denote by D an electronic document that a user wants to sign and by $H(D)$, where H is a hash function, the result of applying the hash function H to D. The creation of the remote qualified electronic signature on $H(D)$ works as follows:

1. The user first authenticates himself to the qualified trust service provider. Strong authentication (e.g., password and OTP generated by an authenticator app on the user's smartphone) is required in order to protect the electronic signature creation data used for electronic signature creation against accidental or malicious use by others.
2. Upon receipt of the authentication request, the QTSP verifies the request and sends its response (either "accepted" or "failed") to the user.
3. The user sends a signature request to the QTSP. This request includes the hash of the document $H(D)$ that the user would like to sign electronically.
4. The QTSP processes the signature request, and creates a qualified electronic signature on $H(D)$ on behalf of the user. The signature is created inside a hardware security module (HSM). The QTSP returns the signature creation result, returned by the signature creation application, to the user. The signature creation result contains the signature of the user on $H(D)$, denoted by $\text{sign}_{\text{User}}(H(D))$, and may contain additional data.

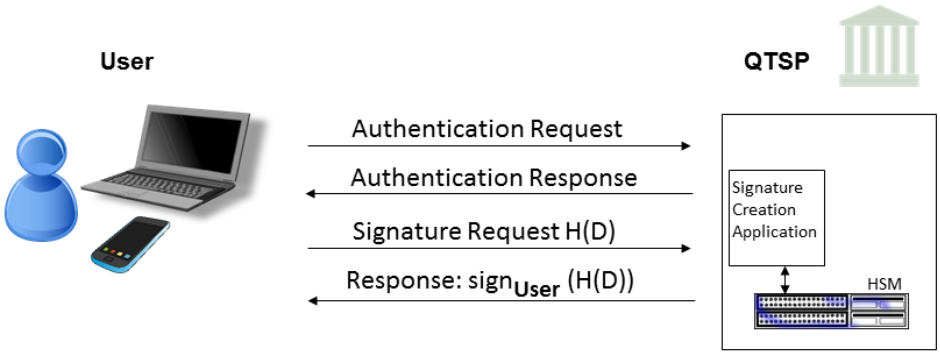


Figure 2.5.: Remote signature creation process

We would like to stress that there are many variants of remote signature creation processes. The remote signature creation process illustrated in Figure 2.5 is only one of

these variants. Another possible variant would be that the user, in Step 3 of the remote signature creation process, sends a signature request to the QTSP which includes the entire document D (and not only the hash of the document $H(D)$).

Requirements for qualified trust service providers. Qualified trust service providers who issue qualified certificates for electronic signature in the case where the electronic signature creation data (that is, private keys) are managed by the qualified trust service provider on behalf of the signatory have to meet the following requirements:

1. The QTSP complies with the applicable requirements of the eIDAS Regulation.
2. The conformity of the qualified electronic signature creation device shall be certified in accordance with Article 30 of the eIDAS Regulation.
3. The QTSP implements the qualified electronic signature creation device in accordance with the conditions of use specified in the Certificate of Conformity of the qualified signature creation device and in the corresponding certification report.
4. The QTSP maintains an up-to-date risk analysis that covers the risks associated with the use of the qualified electronic signature creation device.

Standards. To date there are only very few standards and technical specifications on remote signing services (e.g., CEN/TS 419241:2014 "Security Requirements for Trustworthy Systems Supporting Server Signing"). The European Committee for Standardization (CEN), a European Standardization Organization, is currently developing further standards for remote signing services.

2.3.3.2. Relation between remote signing services and qualified trust services

First, only qualified trust service providers can offer remote signing services to create remote *qualified* electronic signatures where the management, including the generation and storage, of the user's private key is done by the qualified trust service provider [18, Annex II(3)].

Second, the associated qualified trust service to remote signing services to create qualified electronic signatures is the "provision of qualified certificates for electronic signatures". The creation of qualified electronic signatures via a remote signing service is not a qualified trust service.

Identification in the trusted list. The indication that a qualified trust service provider who provides the service "provision of qualified certificates for electronic signatures" (service type = "CA/QC") and manages the private keys on behalf of the users is done in the trusted list via the qualifier "QCQSCDManagedOnBehalf ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf")" [42], which indicates that the private keys associated with the certificates that are issued under this service are residing in a QSigCD "for which the generation and management of that private

key is done by the qualified TSP on behalf of the entity whose identity is certified in the certificate" [42].

2.3.3.3. Advantages and disadvantages of remote signing services.

Compared to the creation of qualified electronic signatures via smart cards or other devices (where the user's private key is stored locally in the device and the signature is created in the device), the creation of remote qualified electronic signatures is convenient and user-friendly, as

- no specific hardware (e.g., smart card, smart card reader, USB stick) is required to create signatures,
- no installation of additional software (e.g., smart card reader driver, middleware) is needed, and
- the creation of electronic signatures is not limited to specific devices or web browsers; the user can typically connect to the remote signing service via any web browser on his laptop, desktop, tablet, or mobile phone.

A disadvantage is that the user has less control over his private key as the key is stored in the QTSP's environment and not locally on a device under the direct control of the user.

Similar to the creation of signatures via smart cards or other devices where the user is responsible for the protection of the device that stores the user's private key and the associated authentication codes (e.g., PIN codes, passwords), the user is responsible for the security of the authentication means (e.g., smart phone, hardware token) and codes (e.g., PIN to unlock the smart phone, passwords) that he uses to authenticate himself to the remote signing server.

2.4. ILNAS Supervision Scheme for qualified trust service providers

In this section, we describe the supervision scheme of ILNAS for qualified trust service providers. In particular, the relationship between the different actors in the supervision scheme will be explained.

Figure 2.6 shows the supervision scheme for qualified trust service providers applied by the ILNAS Digital Trust Department. The supervision scheme relies on the following actors:

- The national accreditation body of a Member state (e.g., the Comité français d'accréditation (COFRAC) in France) that has signed the European cooperation for Accreditation multilateral agreement (EA MLA), accredits the competence of conformity assessment bodies to carry out conformity assessment of a qualified

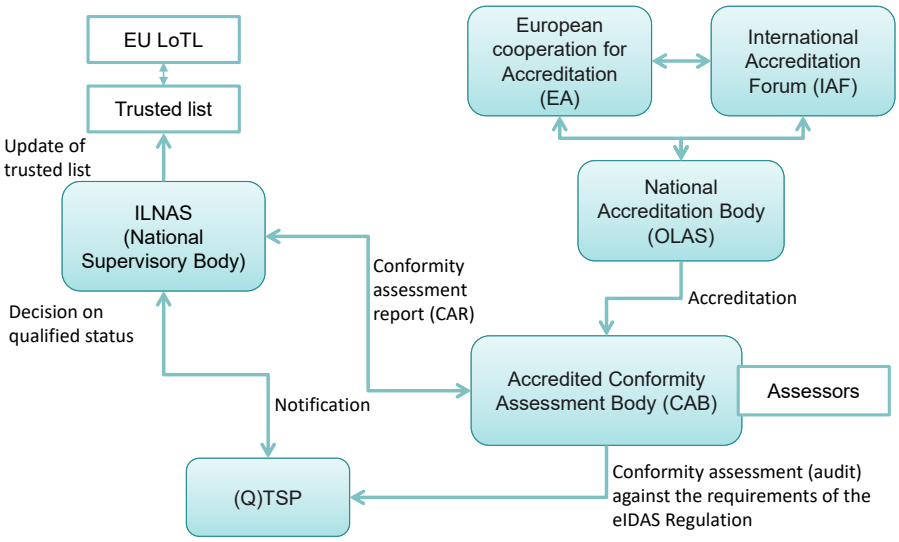


Figure 2.6.: National supervision scheme

trust service provider and the qualified trust services it provides against the requirements of the eIDAS Regulation.[9]

- A conformity assessment body (CAB) is "a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides" [18, Article 3(18)]. Recall that Regulation (EC) No 765/2008 defines a conformity assessment body as a "body that performs conformity assessment activities including calibration, testing, certification and inspection". ILNAS requires that the conformity assessment body is accredited by the national accreditation body of a Member state in accordance with Article 3 (18) of the eIDAS Regulation [18] and recommends that the conformity assessment body is also accredited according to the requirements of the ISO standard ISO/IEC 17065:2012 [28] as well as those in ETSI EN 319403 [19].[10]

- The Digital Trust Department of ILNAS is the supervisory body in Luxembourg, responsible for the supervision of trust service providers, and is also

[9] Note that the national accreditation body in Luxembourg (OLAS) does not perform accreditation regarding the conformity assessment activities related to the eIDAS Regulation.

[10] The European Commission published a list of conformity assessment bodies accredited against the requirements of the eIDAS Regulation (see, [16]).

the body responsible for establishing, maintaining and publishing the national trusted list [33].

- A trust service provider, without qualified status, who intends to start providing qualified trust services, has to submit to the Digital Trust Department of ILNAS a notification of its intention together with a conformity assessment report issued by a conformity assessment body. Further details on the initiation process of a qualified trust service are given in Section 2.4.1.

The national trusted list is a list which includes information about the qualified trust service providers established in Luxembourg and supervised by ILNAS as well as information about the qualified trust services they provide.

2.4.1. Initiation of the Supervision

A trust service provider established in Luxembourg, without qualified status, who intends to start providing qualified trust services, has to submit to the Digital Trust Department of ILNAS a notification of its intention together with a conformity assessment report issued by a conformity assessment body. The notification has to include the completed notification form as well as several documents such as the trust service policies that apply to the trust services for which a qualified status is requested, the termination plan of the TSP and the certificate from the conformity assessment body that demonstrates compliance with the applicable requirements of the eIDAS Regulation. For further details, we refer the reader to the ILNAS procedure for the supervision of QTSPs [27].

The following elements are notably reviewed by the ILNAS upon receipt of a notification by a trust service provider:

- Accreditation of the conformity assessment body;
- Certification and scope of the conformity assessment of the QTSP;
- Coverage of the applicable requirements in the eIDAS Regulation in the conformity assessment report;
- The provided documentation;
- If applicable, the resolution of nonconformities (including corrective actions) detected during the conformity assessment.

If the applicable requirements in the eIDAS Regulation are met by the TSP and the notified trust services, then the qualified status is granted to the TSP and the notified trust services are included in the national trusted list.

If the applicable requirements in the eIDAS Regulation are not met by the TSP or the qualified trust services it intends to provide and if the QTSP fails to resolve non-conformities as requested by the Digital Trust Department of ILNAS, then ILNAS does not grant the qualified status to the TSP. In this case the TSP needs to start the

supervision process again via a new notification to the Digital Trust Department of ILNAS.

It is important to note that, according to Article 21 paragraph (3) of the eIDAS Regulation, qualified trust service providers may only start to provide the trust service for which the qualified status has been requested in the notification after the qualified status has been indicated in the national trusted list.

Tools to support compliance. The conformity assessments shall be carried out against the requirements of the eIDAS Regulation. However, standards and technical specifications can be used as a tool to support the demonstration of compliance to eIDAS requirements. Table 2.3 provides a non-exhaustive list of standards and technical specifications that can be used to demonstrate compliance with requirements in the eIDAS Regulation. References in Table 2.3 are non-specific, meaning that the latest version of the referenced document (including any amendments) applies.

Note however that for some eIDAS requirements there may not (yet) be corresponding requirements in standards. Similarly, for some qualified trust services defined in the eIDAS Regulation (e.g., qualified preservation service for qualified electronic signatures/seals, qualified electronic registered delivery service) there may not (yet) be standards with applicable requirements.

2.4.2. During the Supervision

The supervision shall ensure that the QTSP and its qualified trust services meet the applicable requirements laid down in the eIDAS Regulation. In this regard the certification shall be renewed every two years (via a reassessment audit) and a surveillance audit shall be conducted yearly. Furthermore, an Electronic Data Processing (EDP) audit shall be conducted every two years. ILNAS recommends to conduct the EDP audit with respect to the requirements in the technical specification CEN/TS 419 261:2015 "Security requirements for trustworthy systems managing certificates and time-stamps" [17].

Supervision meetings. During the supervision phase, the Digital Trust Department of ILNAS organises a supervision meeting with each QTSP at least every 6 months, which allows the department to review the recent activities of the QTSP. In particular, the QTSPs that are supervised by ILNAS shall inform ILNAS of any change in the provision of its qualified trust services (e.g., change of subcontractor, change of hardware/software, change of algorithms, intention to cease activities).

Notification of security incidents. According to Article 19 paragraph (2) of the eIDAS Regulation, qualified trust service providers shall, "without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss

Standard/ Techn. Spec.	Scope of TSP activity
ETSI EN 319 401	General policy requirements for trust service providers supporting electronic signatures
ETSI EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements
ETSI EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for Trust service service providers issuing EU qualified certificates
ETSI EN 319 412	Certificate Profiles
ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI EN 319 422	Time-stamping protocol and time-stamp token profiles
ETSI TS 119 312	Cryptographic Suites
CEN/TS 419 241	Security Requirements for Trustworthy Systems Supporting Server Signing
CEN/TS 419 261	Security requirements for trustworthy systems managing certificates and time-stamps
IETF RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol
IETF RFC 2630	Cryptographic Message Syntax

Table 2.3.: Standards and technical specifications to support the demonstration of compliance

of integrity that has a significant impact on the trust service provided or on the personal data maintained therein"[11]. In certain cases, the QTSP also has to notify the customers who are affected by the breach of security or loss of integrity without undue delay.

Ad hoc conformity assessments. Besides the yearly surveillance audit and the two-yearly re-assessment audit, the supervisory body may, according to Article 20 (2) of the eIDAS Regulation, at any time audit or request a conformity assessment body to perform a conformity assessment of a qualified trust service provider at the expense of the trust service provider. The aim of such ad hoc audits is to confirm that the

[11] Note that this requirement encompasses qualified as well as non-qualified trust services provided by the QTSP and that it also applies to non-qualified trust service providers and the non-qualified trust services they provide.

qualified trust service provider and its qualified trust services fulfill the requirements laid down in this eIDAS Regulation. Ad hoc audits can be triggered by the occurrence of events such as:

- Events detected by ILNAS, or
- Events notified by the QTSP to ILNAS, e.g.:
  - Termination of one or more qualified trust services,
  - Changes of policies or procedures of the QTSP,
  - Major changes in the documentation of the QTSP,
  - Change in the provision of one or more qualified trust services,
  - Provision of a new trust service of the same type as trust services already provided but under significantly different policies,
  - Security incidents,
  - Personal data breaches,
  - Complaints.

Depending on the outcome of the ad hoc conformity assessment, ILNAS may update the status of the QTSP or its qualified trust service(s) in the national trusted list.

2.4.3. Termination of the Supervision

The QTSP has to inform ILNAS of its intention to cease one or more of its qualified trust services. In this case, the Digital Trust Department of ILNAS verifies the correct application of the provisions contained in the trust service provider's termination plan, including as to how information is kept accessible in accordance with point (h) of Article 24 paragraph (2) of the eIDAS Regulation. This verification is necessary to maintain the trust and confidence of the affected users in the continuity of the qualified trust services (e.g., the availability of the certificate revocation list) as well as for the purpose of providing evidence in legal proceedings. As an example, suppose that a QTSP ceases all of its activities including the provision of qualified certificates for electronic signatures. If a user wants to validate an electronic signature based on a qualified certificate issued by the trust service provider, where the signature has been created before the cessation of the qualified trust service, then the user must be able to check the status of the certificate at the time of the creation of the signature and, in particular, whether or not the certificate was revoked.

In case of the cessation of some of the qualified trust service provider's qualified trust services, the scope of the supervision by ILNAS changes and the status of the concerned qualified trust services on the national trusted list is updated by ILNAS.

In case of the cessation of all of the qualified trust service provider's qualified trust services, the supervision by ILNAS according to the ILNAS supervision procedure for QTSPs ceases and the status of the trust service provider and of the trust services on the national trusted list is updated by ILNAS.

2.5. Trusted lists

> "Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision." [18, Recital (46)]

Each EU Member State manages a national trusted list which contains information about the qualified trust service providers under its supervision and their qualified trust services. Details on national trusted lists are provided in Section 2.5.1. The national trusted lists contain a pointer to the European List of Trusted Lists (LOTL) which is managed by the European Commission. We provide information on the LOTL and the Trusted List Browser in Section 2.5.2.

2.5.1. National trusted list

The eIDAS Regulation requires EU Member States to establish, maintain and publish trusted lists, which include information about the qualified trust service providers supervised by the supervisory body of the Member State as well as information about the qualified trust services that they provide. Trusted lists not only contain information on currently active qualified trust service providers and the qualified trust services that they currently provide, but also historical information on the trust services that they provide (or that they provided in the past) such as their prior statuses. The lists also include information on trust service providers that have been supervised by the supervisory body in the past as well as information on the trust services that they provided.

Optionally, EU Member States can include in their respective national trusted list information about non-qualified trust service providers and the non-qualified trust services that they provide, provided that this is clearly indicated in the list (see Article 2 of the Commission Implementing Decision (EU) 2015/1505 [8]).

Each national trusted list is digitally signed by the Trusted List Scheme Operator (TLSO), the legal entity in charge of managing the trusted list, to ensure origin authentication of the trusted list. Thus, users are able to verify that a given trusted list was indeed issued by a certain entity.

Under the eIDAS Regulation, national trusted lists have a constitutive value as they present the only reliable source to verify whether a given trust service provider and its trust service had the "qualified" status at a given point in time. A necessary condition for a qualified trust service to benefit from the legal effects associated to it is that the trust service has the "qualified" status in the national trusted list.

As indicated before, trusted lists are mainly used to validate objects (e.g., qualified electronic signatures or qualified timestamps) that have been created by using a qualified trust service. For example, to verify that an electronic signature on a document, created with a public-key certificate, can be considered as a "qualified electronic signature" in the sense of the eIDAS Regulation, one would need to first verify that

- **Qualified status check:** the trust service under which the certificate was issued had the "qualified" status in the trusted list at the time when the signature was

created.[12]

Additional checks include:

- **Suspension and revocation check:** the verification whether the certificate was neither suspended nor revoked at the time of the signature (Certificate Revocation List (CRL) distribution points are included in the certificate),
- **Expiration check:** the verification whether the certificate was not expired at the time of the signature (the expiration date of the certificate is included in the certificate),
- **Cryptographic verification of the digital signature:** the cryptographic verification whether the digital signature is a valid signature on the document, and
- **QSigCD check:** the verification whether the private key corresponding to the certified public key resided in a qualified signature creation device (this information may be included in the trusted list or in the certificate).

The trusted list of Luxembourg includes information about the qualified trust service providers established in Luxembourg and supervised by ILNAS as well as information about the qualified trust services they provide. The Digital Trust Department of ILNAS is Luxembourg's Trusted List Scheme Operator, responsible for maintaining and publishing Luxembourg's trusted list. It is available in three formats HTML, XML, and PDF, and can be accessed on the ILNAS website.[13]

Figure 2.7 shows an extract of the Trusted List Luxembourg when accessed via the Trusted List Browser, a web application made available by the European Commission (see also Section 2.5.2). As shown in Figure 2.7, at the time of writing, LuxTrust S.A. is the only active qualified trust service provider in Luxembourg providing the following qualified trust services (indicated in yellow):

- Qualified certificates for electronic signatures,
- Qualified certificates for website authentication,
- Qualified time stamping service.

The trusted list not only contains information on currently active qualified trust service providers supervised by ILNAS and the qualified trust services that they currently offer, but also historical information on trust service providers that have been supervised by ILNAS in the past.

The trusted list also contains a link to the European List of Trusted Lists (in XML format), information on the trusted list itself such as the date and time when it was

[12] If PKI technology is used, then a trust service is identified on the trusted list via an X.509 certificate in the "Service Digital Identity" field.

[13] URL: https://portail-qualite.public.lu/fr/confiance-numerique/prestataires-services-confiance/liste-confiance.html

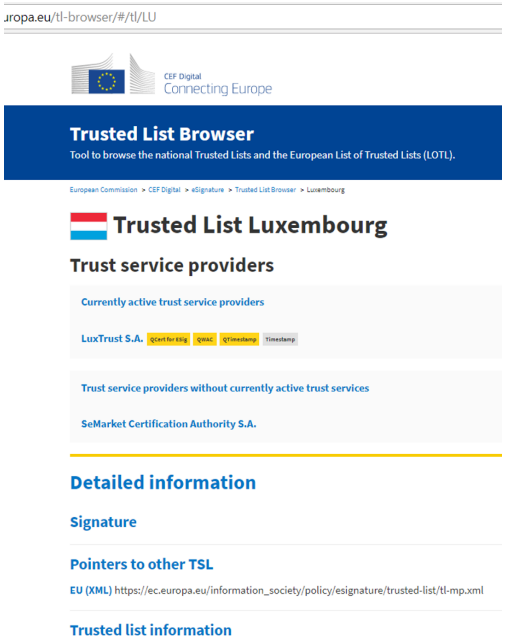


Figure 2.7.: "Trusted List Luxembourg", European Commission, 25th August, 2017. Author's screenshot, 20th February 2018.

issued, the date and time by which an updated trusted list will be issued, as well as a digital signature by the head of the Digital Trust Department of the ILNAS.

Trusted lists have to comply with the technical specifications given in Annex I of the Commission Implementing Decision (EU) 2015/1505 [8]. These technical specifications rely on the requirements in the ETSI Technical Specification 119 612 v2.1.1 [42]. Due to the constitutive value of the trusted lists on which users and applications rely to verify the status of trust services, the trusted lists have to be highly available. More precisely, national trusted lists have to be available 24 hours a day and 7 days a week with a minimum availability of 99,9% over one year, as required by Clause 6.4 of the ETSI Technical Specification 119 612 [42] which is referenced in the Commission Implementing Decision (EU) 2015/1505 [8].

2.5.2. European List of Trusted Lists (LOTL)

According to Article 22 paragraph (4) of the eIDAS Regulation the European Commission makes available information to the public about national trusted lists published by the EU Member States. This information is included in a list, called the European List of Trusted Lists (LOTL). In particular, the LOTL contains pointers to the locations where the national trusted lists of the EU Member States are published. It is available

in a machine-readable format (XML) on the website of the European Commission. [14]

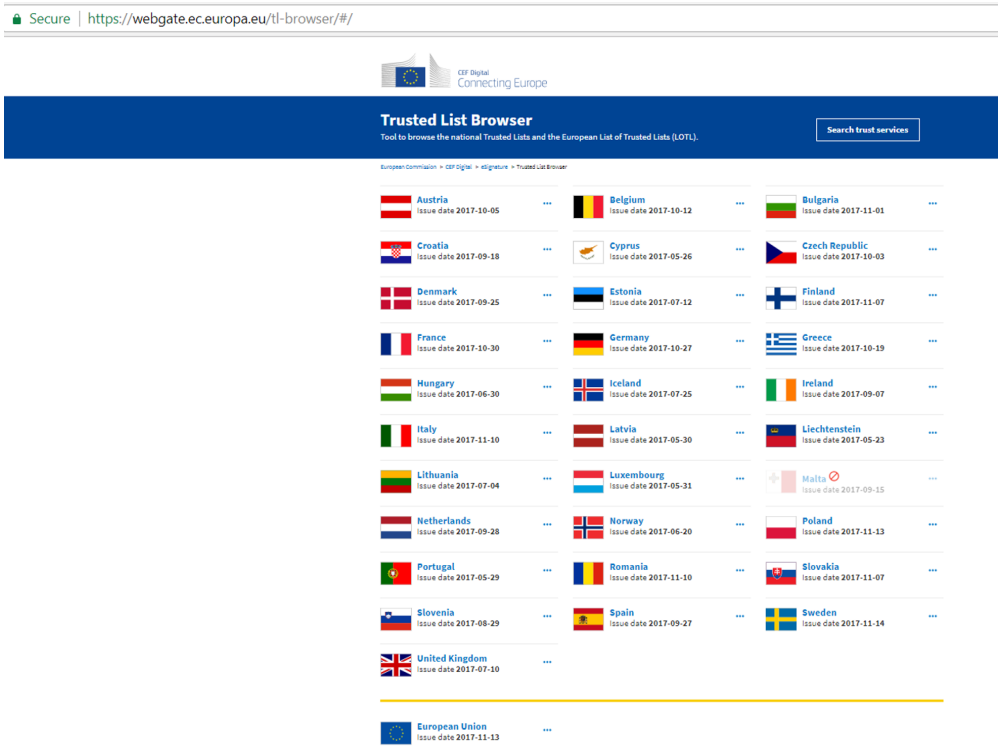


Figure 2.8.: "Trusted List Browser", European Commission, 6th July, 2017. Author's screenshot. 14th November 2017.

In 2017, the European Commission launched the Trusted List Browser [13]. The trusted list browser is a user-friendly web application (see Figure 2.8) that allows users to browse national trusted lists and verify the status of trust services offered by trust service providers established in the European Union or in Norway, Liechtenstein, or Iceland. In particular, users can verify whether a specific trust service offered by some trust service provider had the qualified status at a given point in time.

The European List of Trusted Lists, made available by the European Commission, can be used by users, businesses, and public administrations to validate trust in the objects that were created with the help of qualified trust services (e.g., electronic signatures, electronic seals, electronic timestamps).

In the following section, we illustrate how the software vendor Adobe® integrated information from the European List of Trusted Lists (LOTL) into its software products

[14] `https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml`

Adobe® Acrobat® and Acrobat® Reader® [44, 30] and show how a digital signature based on a qualified certificate for electronic signatures can be validated with Adobe® Acrobat® Reader® software.

2.5.2.1. Application: Adobe European Union Trust List

The "Adobe European Union Trust List" (Adobe® EUTL) is a reduced version of the European List of Trusted Lists (LOTL) as it only includes information on the qualified trust service providers present on the LOTL and information on the qualified trust services provided by them [5]. Non-qualified trust services are excluded from the Adobe® EUTL.

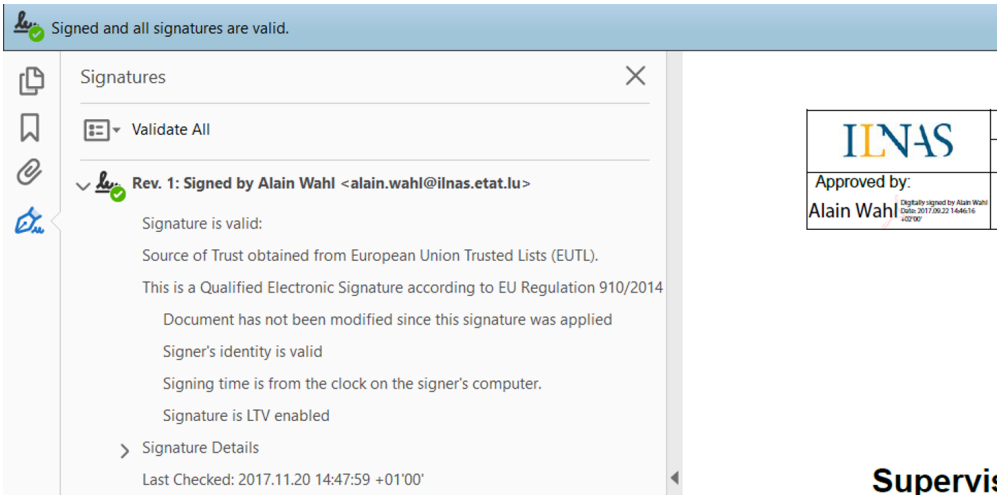


Figure 2.9.: Signature verification for a PDF document with Adobe® software. Author's screenshot, 20th November 2017.

Acrobat® and Acrobat® Reader® software both need to take into account updated information on qualified trust services (such as a change of status or a new qualified trust service) on the European List of Trusted Lists. This is done via an Adobe® server: "Acrobat and Acrobat Reader have been programmed to reach out to an online service run by Adobe to periodically download the list of trusted digital certificates from EU Qualified Trust Service Providers that meet the requirements specified in Article 1 of the Implementing Decision (EU) 2015/1505" [5]. In other words, both of Adobe®'s software products periodically download the trust anchors that correspond to qualified trust services on the LOTL from a server. As a consequence, users can validate digital signatures on electronic documents that have been created using qualified certificates issued under one of these trust anchors. Note that Acrobat® also recognizes whether a digital signature is a qualified electronic signature or a qualified electronic seal according to the eIDAS Regulation and displays this information under

Signature Properties [30].

If a PDF document is digitally signed using a qualified certificate for electronic signatures or electronic seals issued by a qualified trust service provider, then this digital signature can be verified by Adobe® Acrobat® Reader® software. In Figure 2.9 we show how the digital signature on the ILNAS procedure for the supervision of QTSPs can be validated via Adobe® Acrobat® Reader®. Note that Adobe® also indicates that the signature is a qualified electronic signature according to the eIDAS Regulation (which means that the private key corresponding to the certified public key resides in a QSigCD).

We would like to mention that Adobe® Acrobat® and Acrobat® Reader® software not only use the Adobe® EUTL as a source of trust, but also the *Adobe Approved Trust List* (AATL) which includes certification authorities established outside of the EU (e.g., DigiCert in the US or SwissSign in Switzerland) [4]. Hence, digital signatures based on a certificate that has been issued under one of the certification authorities on the AATL can be validated as well with Adobe® Acrobat® and Acrobat® Reader® software.

3. Conclusion

In this document we presented the different trust services and qualified trust services introduced by the eIDAS Regulation. Compared to non-qualified trust services, qualified trust services can only be provided by *qualified* trust service providers. In addition, qualified trust services have to meet stricter requirements than non-qualified trust services. In particular, when a trust service provider established in Luxembourg intends to start providing a qualified trust service, it has to submit to ILNAS (Digital Trust Department) a notification of its intention, a conformity assessment report issued by a conformity assessment body, as well as additional information required by ILNAS. Furthermore, for each of the qualified trust services, we provided a range of use cases where the qualified trust service can be used in practice.

Then, in Section 2.4, we described the ILNAS Supervision Scheme for qualified trust service providers. As explained before, qualified trust service providers may only start to provide the trust service for which the qualified status has been requested in the notification after the qualified status has been granted by ILNAS and after this status has been indicated in the national trusted list.

Finally, in Section 2.5, we provided information on the national trusted list. The national trusted list (as well as the list of trusted lists) can be used to validate trust in electronic signatures or seals, for instance.

We hope that industry will use trust services and, in particular, qualified trust services to improve the security of their applications and to strengthen user trust and confidence in their digital transactions. We encourage individuals to use trust services, in particular, qualified certificates for electronic signatures and qualified electronic time stamping to sign, respectively, time stamp electronic documents, especially in a cross-border context within the European Union.

It will be interesting to see how the market of trust services, and more generally, the provision of services that confer or improve trust in digital transactions, will evolve in the future. In the following we highlight some developments in this area:

- **Alternative identification methods:** Before a qualified trust service provider issues a qualified certificate to a user, he first verifies the identity of this user. Traditionally, this verification of the user's identity (via its identity card or passport) is done by the physical presence of the user at a registration authority. The eIDAS Regulation permits various other identification methods to be used by the qualified trust service provider; for example:
  - an identification method based on the use of a qualified certificate for electronic signatures that has been issued after identity verification by physical presence (see Article 24(1) letter (c) of the eIDAS Regulation), or

– an identification method that is recognised at national level and provides an equivalent assurance in terms of reliability to physical presence (see Article 24(1) letter (d) of the eIDAS Regulation). The equivalent assurance has to be confirmed by a conformity assessment body.

The use of these alternative identification methods would allow a qualified trust service provider to not only provide its qualified trust services in the country where it is established and where its registration authorities are located, but also in other EU countries.

- **New technologies:** Trust in electronic transactions can also be conferred using new technologies. For example, time stamps can be created in a decentralized way using blockchain [26, 45]. The authors of [26] have implemented their timestamping concept in the timestamping web service *OriginStamp*[1], which uses the decentralized Bitcoin blockchain to store time stamps. We refer the reader to [31] for a comparison between traditional timestamping methods and timestamping methods based on blockchain.

  Certificates for website authentication and (qualified) time stamps may be used in the context of TLS-N [39]. TLS-N is an extension of TLS which allows the generation of *non-repudiable* proofs of the conversation contents of a TLS session. These proofs can afterwards be verified by third parties. The certificate chain is one element that is included in the proof; in case a qualified certificate for website authentication is used, the verification of this element could be done using the list of trusted lists (LOTL). As mentioned in [39], "in order to retrospectively understand the time of validity of a proof, either the generator or the validator could make use of a timestamping service attesting the existence of the proof". Here either a non-qualified or a qualified timestamping service provided by a (qualified) trust service provider could be used to establish that the proof existed at that time.

Acknowledgements. ILNAS would like to thank Mr Lionel Antunes (Centre des Technologies de l'Information de l'Etat (CTIE)) for his valuable comments on this document.

[1] https://app.originstamp.org/home

Bibliography

[1] Specialist Task Force 523: Standards for eIDAS trust services – electronic registered delivery and registered electronic mail. Available from https://portal.etsi.org/STF/stfs/STFHomePages/STF523 (accessed on 19/02/2018.

[2] Specialist Task Force 524: Standards for eIDAS trust services including electronic signatures – trust services for validation. Available from https://portal.etsi.org/STF/stfs/STFHomePages/STF524 (accessed on 19/02/2018).

[3] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017, October 6 2017. Available from https://www.eu2017.ee/news/insights/tallinn-declaration-egovernment-ministerial-meeting-during-estonian-presidency (accessed on 8/1/2018).

[4] Adobe. Adobe Approved Trust List members, October 2017. Available from https://helpx.adobe.com/lu_en/acrobat/kb/approved-trust-list1.html (accessed on 20/11/2017).

[5] Adobe. Adobe Trust Services, 3 November 2017. Available from https://helpx.adobe.com/acrobat/kb/trust-services.html (accessed on 20/11/2017).

[6] A-SIT Secure Information Technology Centre Austria. Browser Addon for Certificate Validation using EU Trust Lists, February 2017. Available from https://demo.a-sit.at/browser-addon-for-certificate-validation-using-eu-trust-status-lists-tsl/ (accessed on 8/1/2018).

[7] European Banking Authority. Final report draft regulatory technical standards on strong customer authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). Available from https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 (accessed on 8/1/2018).

[8] European Commission. COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *OJ*, L 235:26–36, 2015. Available from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0005.

[9] European Commission. Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *OJ*, L 235:37–41, 2015. Available from `https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:JOL_2015_235_R_0006`.

[10] European Commission. Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services. *OJ*, L 128:13–15, 2015. Available from `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0806`.

[11] European Commission. Commission Implementing Decision (EU)2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices. *OJ*, L 109:40–42, 2016. Available from `http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.109.01.0040.01.ENG`.

[12] European Commission. eIDAS Regulation Questions and Answers on rules applicable to Trust Services as of 1 July 2016, 2017. Available from `http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=48353` (accessed on 18/12/2017).

[13] European Commission. Trusted list browser now available, July 2017. Available from `https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2017/07/05/Trusted+List+Browser+Now+Available` (accessed on 14/11/2017).

[14] European Commission. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication C/2017/7782, 2018. Available from `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN`.

[15] European Commission. Compilation of Member States notification on SSCDs and QSCDs. Available from `https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds`.

[16] European Commission. List of conformity assessment bodies (CABs) accredited against the requirements of the eIDAS regulation. Available from `https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation`.

[17] European Committee for Standardization (CEN). CEN/TS 419 261:2015 Security requirements for trustworthy systems managing certificates and

time-stamps. Available from https://ilnas.services-publics.lu/ecnor/displayStandard.action?id=118703.

[18] European Parliament Council of European Union. Regulation EU no 910/2014 of the European Parliament and of the Council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *OJ*, L 257:73–114, 2014. Available from http://eur-lex.europa.eu/eli/reg/2014/910/oj.

[19] European Telecommunications Standards Institute. *ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers*. European Telecommunications Standards Institute, France, 2015.

[20] European Telecommunications Standards Institute. *ETSI SR 019 050 V1.1.1 (2015-06) Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures*. European Telecommunications Standards Institute, France, 2015.

[21] European Telecommunications Standards Institute. *ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation*. European Telecommunications Standards Institute, France, 2016.

[22] European Telecommunications Standards Institute. *Draft ETSI TS 119 441 V0.0.4 (2017-11) Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services*. European Telecommunications Standards Institute, France, 2017. Available from https://docbox.etsi.org/esi/open/Latest_Drafts/ESI-0019441v004.pdf (accessed on 17/1/2018).

[23] European Telecommunications Standards Institute. *ETSI EN 319 412 V2.2.1 (2017-11) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*. European Telecommunications Standards Institute, France, 2017.

[24] European Commission Directorate-General for Financial Stability Financial Services and Capital Markets Union. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN CENTRAL BANK, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Consumer Financial Services Action Plan: Better Products, More Choice, COM/2017/0139 final, 23/03/2017. Available from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0139.

[25] CA/Browser Forum. Guidelines for the issuance and management of extended validation certificates. Available from https://cabforum.org/extended-validation/.

[26] B. Gipp, N. Meuschke, and A. Gernandt. Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. *Proceedings of the iConference 2015, Newport Beach, CA, USA*, 2015. Available from `http://ischools.org/the-iconference/`.

[27] ILNAS – Digital Trust Department. ILNAS/PSCQ/Pr001 – Supervision of qualified trust service providers (QTSPs). Available from `https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/confiance-numerique/surveillance-psc/procedures/ilnas-pscq-pr001-supervision-en/ilnas-pscq-pr001-supervision-en.pdf`.

[28] International Organization for Standardization. *ISO/IEC 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services*. International Organization for Standardization. Geneva, Switzerland, 2012.

[29] ISO/IEC. *ISO/IEC 9798-1:2010: Information technology – Security techniques – Entity authentication – Part 1: General*. International Organization for Standardization, Geneva, Switzerland, 2010.

[30] John Jolliffe and Andrea Valle. E-Signatures: Unsung Hero of the EU's Digital Single Market, 10 May 2016. Available from `https://blogs.adobe.com/policy/2016/05/10/e-signatures-unsung-hero-of-the-eus-digital-single-market/` (accessed on 20/11/2017).

[31] Shawn M. Jones. 2017-04-20: Trusted Timestamping of Mementos, April 20 2017. Available from `https://ws-dl.blogspot.lu/2017/04/2017-04-20-trusted-timestamping-of.html` (accessed on 11/12/2017).

[32] Legilux. Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques et portant modification de 1) l'article 104 du code civil; 2) la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales; 3) la loi communale modifiée du 13 décembre 1988; 4) la loi électorale modifiée du 18 février 2003 et abrogeant 1) la loi modifiée du 22 décembre 1886 concernant les recensements de population á faire en exécution de la loi électorale et 2) l'arrêté grand-ducal du 30 aoùt 1939 portant introduction de la carte d'identité obligatoire., June 2013. Available from `http://legilux.public.lu/eli/etat/leg/loi/2013/06/19/n3/jo`.

[33] Legilux. Loi du 4 juillet 2014 portant réorganisation de l'institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services et portant organisation du cadre général pour la surveillance du marché dans le contexte de la commercialisation des produits, July 2014. Available from `http://legilux.public.lu/eli/etat/leg/loi/2014/07/04/n2/jo`.

[34] Legilux. Règlement grand-ducal du 21 septembre 2017 modifiant le règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique, August 2015. Available from `http://legilux.public.lu/eli/etat/leg/rgd/2017/09/21/a865/jo`.

[35] Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec, and Vashek Matyas. The return of Coppersmith's attack: Practical factorization of widely used rsa moduli. In *24th ACM Conference on Computer and Communications Security (CCS'2017)*, pages 1631–1648. ACM, 2017.

[36] National Archives of Australia. Digital preservation planning, 2017. Available from `http://www.naa.gov.au/information-management/managing-information-and-records/preserving/digi-pres-planning.aspx` (accessed on 12/12/2017).

[37] European Parliament Council of the European Union. DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. *OJ*, L 013:12–20, 1999.

[38] European Parliament Council of the European Union. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. *OJ*, L 337:35–127, 2015.

[39] Hubert Ritzdorf, Karl Wuest, Arthur Gervais, Guillaume Felley, and Srdjan Capkun. TLS-N: Non-repudiation over TLS Enabling - Ubiquitous Content Signing for Disintermediation. Cryptology ePrint Archive, Report 2017/578, 2017. Available from `https://eprint.iacr.org/2017/578`.

[40] John Erik Setsaas. Blog: Introduction to digital seals, 24 October 2016. Available from `https://www.signicat.com/blog/blog-introduction-digital-seals/` (accessed on 29/11/2017).

[41] Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov, Alex Petit Bianco, and Clement Baisse. Announcing the first SHA1 collision, February 23 2017. Available from `https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html` (accessed on 11/12/2017).

[42] European Telecommunications Standards Institute. *ETSI TS 119 612 V2.1.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Trusted Lists*. European Telecommunications Standards Institute, France, 2015.

[43] European Telecommunications Standards Institute. *ETSI SR 019 510 V1.1.1 (2017-05) Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures*. European Telecommunications Standards Institute, France, 2017.

[44] Andrea Valle. EU Trusted List now available in Adobe Acrobat!, 26 October 2015. Available from Adobe Document Cloud blog: https://blogs.adobe.com/documentcloud/eu-trusted-list-now-available-in-adobe-acrobat/ (accessed on 20/11/2017).

[45] Karl Wüst and Arthur Gervais. Do you need a Blockchain? Cryptology ePrint Archive, Report 2017/375, 2017. Available from https://eprint.iacr.org/2017/375.

Index

A. Appendix

A.1. Background on qualified certificates in the context of the PSD2 Directive

A major objective of the PSD2 Directive is to introduce enhanced security standards for online transactions. The adoption and implementation of these standards by payment service providers will strengthen the security of online transactions and hence enhance consumer confidence and trust.

The PSD2 Directive states in its Article 98 paragraph 1 that the European Banking Authority (EBA) shall, in close cooperation with the ECB and after consulting all relevant stakeholders, develop draft regulatory technical standards on authentication and communication addressed to payment service providers [38]. More precisely, it states that the "EBA (European Banking Authority) shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:

(a) the requirements of the strong customer authentication referred to in Article 97(1) and (2);

(b) the exemptions from the application of Article 97(1), (2) and (3), based on the criteria established in paragraph 3 of this Article;

(c) the requirements with which security measures have to comply, in accordance with Article 97(3) in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials; and

(d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers." [38, Article 98(1)]

Article 98 paragraph 2 of the PSD2 Directive enumerates the objectives of the draft regulatory technical standards: "The draft regulatory technical standards referred to in paragraph 1 shall be developed by EBA in order to:

(a) ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements;

(b) ensure the safety of payment service users' funds and personal data;

(c) secure and maintain fair competition among all payment service providers;

(d) ensure technology and business-model neutrality;

(e) allow for the development of user-friendly, accessible and innovative means of payment." [38]

In accordance with Article 98 paragraph 1 of the PSD2 Directive, the EBA has developed, in close cooperation with the European Central Bank (ECB), draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication [7]. The European Commission can adopt regulatory technical standards based on the draft developed by the EBA in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010 [38, Article 98(4)].

In November 2017 the European Commission has published Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing PSD2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [14]. This Regulation integrates the regulatory technical standards developed by the EBA with some amendments.

One of the requirements in [14] is that "For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation [14, Article 34(1)].

The rules in the PSD2 Directive apply from 13 January 2018. Regulation (EU) 2018/389 of 27 November 2017 supplementing PSD2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [14] will become applicable in September 2019.

A.2. Comparison between qualified certificates for website authentication and extended validation certificates

Qualified certificates for website authentication (QWACs) are similar to extended validation (EV) certificates in terms of security guarantees provided with respect to the identity of the entity who controls a certain website.

The purposes of both types of certificates are to:

- identify the entity that controls a website so that a visitor of the website can be sure that he is accessing the intended website,

- enable encrypted communication between the visitor of the website and the website (e.g., via TLS),
- strengthen the security of electronic transactions with the website.

The main differences between the two types of certificates are the following:

- **Certificate issuance:** Whereas EV certificates can only be issued to legal persons (see [25])[1], QWACs can be issued to natural or legal persons (see [18, Annex IV]).
- **Identity verification:** The requirements on the verification of the legal existence and identity of the entity who requests a certificate are different. The EV guidelines require that "A Principal Individual[2] associated with the Business Entity MUST be validated in a face-to-face setting" [25] by the certificate authority or the registration agency. In contrast, the eIDAS Regulation requires the qualified trust service provider to use one of the four methods specified in its Article 24 paragraph 1 to verify the identity of the entity to whom the certificate is to be issued. These methods include the physical presence of the entity as well as other identification means such as certain electronic identification means or methods that are recognised at national level and provide equivalent assurance in terms of reliability to physical presence [18].
- **Requirements:** The EV guidelines require that "The CA MAY issue EV Certificates, provided that the CA and its Root CA satisfy the requirements in these Guidelines and the Baseline Requirements". In contrast, a trust service provider who would like to issue QWACs has to meet all the applicable requirements in the eIDAS Regulation; these requirements include, for example, the obligation to notify security incidents to the supervisory body and to undergo regular audits (at least every 24 months) by a conformity assessment body with respect to the applicable requirements in the eIDAS Regulation.
- **Supervision:** In contrast to CAs who provide EV certificates, a trust service provider who would like to issue QWACs falls under the supervision of a supervisory body. We refer the reader to Section 2.4 for details on the ILNAS supervision scheme for qualified trust service providers. Recall that a trust service provider may only start to provide QWACs after the qualified status has been attributed to the trust service provider and the notified QWAC trust service is indicated in a national trusted list.

[1] According to CA/Browser Forum EV guidelines, "The CA MAY only issue EV Certificates to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements specified below" [25].

[2] A Principal Individual is defined as "An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of EV Certificates" [25].

- **Maximum validity period:** Whereas the eIDAS Regulation does not contain specific requirements on the validity period for QWACs, the EV Guidelines require that "The validity period for an EV Certificate SHALL NOT exceed 825 days. It is RECOMMENDED that EV Subscriber Certificates have a maximum validity period of twelve months." [25].

If a qualified trust service provider satisfies the requirements in the eIDAS Regulation and, in addition, those in the EV Guidelines, he may issue both types of certificates. He may also issue certificates to legal persons that are EV certificates as well as QWAC certificates as long as these certificates satisfy the applicable requirements in the eIDAS Regulation and the EV Guidelines.

ILNAS
Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -50 · Fax : (+352) 24 79 43 -50 · E-mail : confiance-numerique@ilnas.etat.lu

www.portail-qualite.lu